



TYPHOON

- GREENFIELD DEVELOPMENT LIMITED -

ANTI-MONEY LAUNDERING/COMBATING FINANCIAL TERRORISM POLICY AND PROCEDURES

These are the Anti-Money Laundering (ALM) Policy and procedures adopted by Typhoon Greenfield Development Ltd in compliance with the Anti-Money Laundering Act 2020 (1044). The business will actively prevent and take measures to guard against being used as a medium for money laundering activities and terrorism financing activities and any other activity that facilitates money laundering or the funding of terrorist or criminal activities.

To these ends:

- The identities of all new and existing clients will be verified to a reasonable level of certainty.
- A risk-based approach will be taken to the monitoring of client tax and accounting affairs.
- Any suspicious activity will be reported, and all AML activities recorded.
- A Money Laundering Reporting officer (MLRO) shall be appointed to coordinate the AML policies and procedures of the business.
- All staff that meet or contact clients and potential clients of this firm are required to acknowledge that the policy and procedures have been read and understood before meeting or contacting clients.

ANTI-MONEY LAUNDERING PROCEDURES FOR TYPHOON GREENFIELD DEVELOPMENT LTD

1. CUSTOMER DUE DILIGENCE

The business has established a Know-Your-Client (KYC) policy to ensure that the identities of all new and existing clients are verified to a reasonable level of certainty. This will include all individual clients, all directors, and shareholders with a stake holding of 25% or more of client companies, all partners of client partnerships, and every board member of client charities. Identities will be verified online, through government agencies, and/or face-to-face.

Online identity verification agencies, which use data from multiple sources over a period of time, will also be used for international clients. These commercial agencies must have processes that allow the enquirer to capture and store the information they used to check and verify an identity.

The following documentation may be presented by the individual:

- Either a passport, driver's license, or government issued document featuring a matching photograph of the individual, and a full name and date of birth matching those Provided.
- An original recent utility bill, or government issued document with the same address matching those provided by the individual.

If the business fails to verify a client's identity with reasonable certainty, it will not establish a business relationship or proceed with the transaction. If a potential or existing client either refuses to provide the information described above when requested, or appears to have intentionally provided misleading

HNO. OTB. 602 Main Market, Adum, Kumasi
info@typhest.com | www.typhest.com

Typhoon Greenfield Development Ltd | Registration no: CS304062018

information, the business shall refuse to commence a business relationship or proceed with the transaction requested.

2. RISK ASSESSMENT AND ONGOING MONITORING

The business shall take a risk-based approach in monitoring the financial activities of its clients. The business will actively not accept high-risk clients that are identified as follows:

- Clients based in or conducting business in or through, a high-risk jurisdiction.
- Money sent to or received from areas known to have high levels of criminality or terrorist activity.
- Upstream companies who are known to be active in a higher-risk business activity such as arms, gaming and casino industry, antiques and art, sects, and their leaders.
- Gold-Supplying Counterparties whose mined gold is claimed to have originated from a country that has limited known reserves, likely resources or expected production levels of gold.

The business will conduct ongoing monitoring of business relationships with customers, to ensure that the documents, date or information held evidencing the customer's identity are kept up to date.

The following are examples of changes in a client's situation that may be considered suspicious:

- Uncharacteristic transactions which are not in keeping with the customer's known activities.
- Peaks of activity at particular locations or at particular times.
- Unfamiliar or untypical types of customers or transactions.

Whenever there is cause for suspicion, the client will be asked to identify and verify the source or destination of the transactions, whether they be individuals or company beneficial owners.

No action need be taken if there is no cause for suspicion.

3. INTERNAL CONTROLS AND COMMUNICATION

The compliance officer also acts as the MLRO. Internal controls and communication shall be escalated and approved by senior management.

4. MONITORING AND MANAGING COMPLIANCE

The MLRO will regularly monitor the following procedures to ensure they are being carried out in accordance with the AML policies and procedures of the business:

- client identity verification.
- Reporting suspicious transactions.
- record keeping.

The MLRO will also monitor any developments in the MLR and the requirements of the MLR supervisory body. Changes will be made to the AML policies and procedures of the business when appropriate to ensure compliance.

5. SUSPICIOUS ACTIVITY REPORTING

A Suspicious Activity Report (SAR) will be made to the Financial Intelligence Centre (FIC) as soon as the knowledge or suspicion that criminal proceeds exist arises. The MLRO will be responsible for deciding whether the suspicion of illegal activity is great enough to justify the submission of a SAR.

Further details on FIC can be found at:

<https://fic.gov.gh/>

6. RECORD KEEPING

Records of all identity checks will be maintained for up to 5 years after the termination of the business relationship or 5 years from the date when the transaction was completed. The business will ensure that all documents, data or information held in evidence of customer identity are kept up to date.

Copies of any SAR, together with any supporting documentation filed will be maintained for 5 years from the date of filing the SAR.

All records will be handled in confidence, stored securely, and will be capable of being retrieved without undue delay.

7. TRAINING

All affected employees are provided with training that explains the Money Laundering ACT 2008, ACT (749) and how they affect the firm, its clients, and its employees.

All affected employees are trained on their responsibilities in relation to money laundering legislation and are aware of how to identify and deal with transactions that may involve money laundering.



K.A. Nsiah-Asare
Chief Executive Officer